Никак по нотам

ТОМ 17

РОССИЯ В ГЛОБАЛЬНОЙ ПОЛИТИКЕ

№ 2 • МАРТ – АПРЕЛЬ • 2019

ISSN 1810-6439

9 771810 643008 >

ИЗДАЕТСЯ ПРИ УЧАСТИИ
FOREIGN AFFAIRS

ТОМ 17

РОССИЯ В ГЛОБАЛЬНОЙ ПОЛИТИКЕ

№ 2 • МАРТ – АПРЕЛЬ • 2019

«Все позволено» и новая уязвимость

Почему проблема киберугроз становится главной в международной безопасности

Владимир Орлов

Дело было без малого два десятилетия назад. Мне принесли рукопись книги. Называлась она «Информационные вызовы национальной и международной безопасности». Это сейчас проблематика международной информационной безопасности (МИБ) – или «кибербезопасности», как ее, сильно упрощая, еще называют – у всех на слуху и находится в топе глобальных угроз. А тогда о МИБ не то чтобы никто не говорил: говорили, конечно, особенно в узких экспертных кругах, но как-то «через запятую», и эта проблема оказывалась на заднем плане. А вскоре случилось 11 сентября, и угроза международного терроризма на время затмила все остальные.

ЛИСТАЯ СТАРЫЕ СТРАНИЦЫ

Но достаточно было пролистать принесенную мне рукопись, как я понял: речь идет об аналитическом труде неординарного калибра. И о глобальной угрозе масштаба гораздо большего, чем мне самому казалось до той поры. Особенное внимание уделялось сценариям кибервойн… хотел сказать «кибервойн будущего», однако авторы справедливо обращали внимание, что это уже «войны настоящего». Они предупреждали о возможности перерастания киберконфликта в ракетно-ядерный и были убеждены,

В.А. Орлов – профессор кафедры прикладного анализа международных проблем МГИМО МИД России, заведующий Центром глобальных проблем и международных организаций Дипломатической академии МИД России; основатель ПИР-Центра.

что при двустороннем вооруженном конфликте непредсказуема реакция стороны, подвергшейся воздействию информационного оружия: «Может сложиться ситуация, когда выявление факта применения информационного оружия даже в очень ограниченном масштабе может привести к "испугу" и предположению, что вскрыта только "вершина айсберга" информационной атаки. Вслед за таким выводом может последовать ограниченное или массированное применение ядерного оружия». «Запретить разработку и использование информационного оружия на нынешнем этапе вряд ли удастся, как это сделано, например, для химического или бактериологического оружия, – делали авторы неутешительный вывод. – Понятно также, что ограничить усилия многих стран по формированию единого глобального информационного пространства невозможно. Поэтому развязки возможны только на пути заключения разумных соглашений, опирающихся на международное право и минимизирующих угрозы применения информационного оружия».

Рукопись я тогда без промедления опубликовал, и вышедшая книга не прошла незамеченной. (Информационные вызовы национальной и международной безопасности. Под ред. А.В. Федорова и В.Н. Цыгичко. М.: ПИР-Центр, 2001.)

ГОЛЫЕ И НАПУГАННЫЕ

За годы, прошедшие с тех пор, информационные технологии шагнули далеко вперед. Интернет стал сродни кислороду: отключи – и люди задохнутся; зависимость от интернета сделалась тотальной. Об информационных войнах теперь не пишет только ленивый, а среди студентов-международников желающих писать выпускные работы про «кибер» гораздо больше, чем про «ядерку». В ООН не один год заседала Группа правительственных экспертов (ГПЭ), обеспокоенных проблематикой МИБ. Используя название известного телешоу, можно сказать, что простые люди чувствуют себя перед угрозами, исходящими из информационного пространства, «голыми и напуганными». «Голые» – потому что ничем не защищены. «Напуганные» – потому что знают, что ничем не защищены. Страх и растерянность, граничащие с паникой и паранойей, то и дело окутывают, будто смог, целые страны.

Несмотря на все это, воз и ныне там. Международное сообщество ни на йоту не приблизилось к выработке того, что могло бы стать «киберДНЯО» – юридически обязывающим договором о нераспространении кибероружия, который поставил бы заслон перед информационными войнами. «Это невозможно. В отличие от ядерного оружия, в случае с кибероружием мы далеко не всегда сможем идентифицировать источник атаки. Больше того, мы почти никогда не будем в состоянии отделить государственные субъекты от негосударственных», – разводят руками маститые эксперты – участники Московской конференции по международной безопасности (*MCIS*). Правда, не менее именитые коллеги не видят тут ничего невозможного: «Я бы предложила создать (…) международную конвенцию по нераспространению кибероружия и признанию невозможности для всех стран распространения кибероружия, – заявила Наталья Касперская, президент группы компаний *InfoWatch*. – Необходимо говорить об этом и стремиться к этому, чтобы все страны, особенно ведущие, такую конвенцию подписали».

В качестве компромисса (либо первого шага по преодолению «кибербеспредела») выдвигаются идеи по выработке международных «кодексов поведения» в киберпространстве. Например, «Парижский призыв к обеспечению доверия и безопасности в киберпространстве», оглашенный в ноябре 2018 г. президентом Франции, или документ по международным нормам кибербезопасности, представленный в 2014 г. корпорацией *Microsoft* на саммите *Global Cyberspace Cooperation* в Берлине.

Действительно, первый шаг делать надо, и он не обязательно должен быть юридически обязывающим и всеобъемлющим, хотя и важно, чтобы уже на первом этапе были представлены интересы различных регионов мира. Однако общая слабость «мер по укреплению доверия» и «кодексов поведения» – аморфность, неверифицируемость и необязательность для исполнения. ДНЯО – крупнейший международный договор XX века, ставший краеугольным камнем глобальной безопасности – тем и силен, что близок к всеохватности: в его юрисдикции – 192 государства планеты. Глобальный характер информационных угроз требует и глобального ответа: договора, столь же авторитетного и универсального, каким в ядерной области является ДНЯО.

В этих условиях не окончательным решением, но весомым шагом на пути к нему могли бы стать двусторонние соглашения между ключевыми субъектами информационного пространства. Однако кризис в системе договоров по контролю над вооружениями, который мы сегодня наблюдаем и который на наших глазах усугубляется, не позволяет говорить о реалистичности таких двусторонних юридически обязывающих соглашений в информационной сфере (или, если угодно, в области кибероружия), по крайней мере на ближайшую перспективу.

Значит, все позволено? Соблазнительный вывод. Потому что как раз чувство вседозволенности пьянит. Оно развращает. О масштабах американских операций в киберпространстве мы догадывались и раньше. Но благодаря разоблачениям Эдварда Сноудена, сделанным в июне 2013 г., кое-что из тайного стало явным. Степень американского (и британского) кибервмешательства по всему миру беспрецедентна. Основной мишенью информационных атак американского государства оказалась горстка еще не только де-юре, но и де-факто суверенных государств, проводящих независимую внешнюю политику. Так, США неоднократно – и в основном успешно – применяли кибероружие против Ирана, в том числе и против его мирной ядерной инфраструктуры.

Но все-таки центральным объектом для американских информационно-кибернетических операций была и остается Россия. Согласно оценке, прозвучавшей в феврале с.г. из Кремля, «территория США постоянно используется для организации огромного количества кибератак против различных российских структур. Это – реальность, в которой мы живем». Характерен заголовок статьи в свежем номере авторитетного Бюллетеня атомных ученых, выходящего в США: «Кибератаки против России – государства с самым большим ядерным арсеналом – представляют глобальную угрозу» .

НОВАЯ УЯЗВИМОСТЬ

Летом 2018 г. я пересек девятнадцать американских штатов. Говорил с простыми людьми где-нибудь в Оклахоме или в Вайоминге. Пытался разобраться, что тревожит «одноэтажную Америку». И как простые американцы относятся к России. А относятся они

к России в основном или хорошо, или никак. Никакой «русофобии», которой страдают вашингтонские элиты, я в американской глубинке не заметил. Правда, если при наших разговорах был выключен телевизор. Но вот если телевизор был как назло включен – и не на спортивных каналах, а на новостных, – тогда в наши разговоры начинали вклиниваться совершенно сюрреалистичные мотивы: «российской угрозы», «вмешательства России в американские выборы», «косвенного контроля со стороны России за многими местными американскими СМИ», «коварства Кремля» и т.п. Но если русофобии в американской глубинке я не встретил, то ощущение уязвимости вполне. И здесь глубинка вполне совпадает с Вашингтоном, хотя в столице это ощущение уязвимости еще острее. С чего бы?

16 июля 1945 г. Соединенные Штаты обрели монополию на ядерное оружие, когда в Аламогордо провели испытание атомной бомбы под кодовым названием «Троица». Но чувство монополии и безнаказанности не прошло и после 29 августа 1949 г., когда атомную бомбу испытал Советский Союз. Вроде бы исключительность США в ядерных вооружениях была подорвана, однако еще несколько лет разрыв в ядерных арсеналах двух стран был столь велик (и настолько в пользу Соединенных Штатов), что комфорт сохранялся. И даже когда СССР стал сокращать разрыв, совершенствовать точность и дальность ракетных носителей, даже когда он 30 октября 1961 г. испытал на Новой Земле водородную «царь-бомбу», – и тогда Вашингтон не воспринимал Москву в ядерном соревновании на равных, ощущая себя уверенно и защищенно.

Понадобился Карибский кризис октября 1962 г., появление советских ракет и ядерного оружия на Кубе, в «подбрюшье» США, чтобы до американского руководства дошло: мир изменился. Ядерной неуязвимости Соединенных Штатов больше нет и не будет. Надо отдать должное президенту Джону Кеннеди. Когда читаешь стенограммы совещаний в Белом доме в дни Карибского кризиса, видишь, как день за днем президент мужает, тщательно вникает в ситуацию, вникнув, удерживает министров и советников от сползания к ядерной войне, находит в себе силы для компромисса. И это несмотря на огромное внутриполитическое

давление, на призывы «показать себя с русскими пожестче», «ответить со всей мощью», ведь Карибский кризис разворачивался за считанные дни до промежуточных выборов в Конгресс.

Уроки были извлечены. Через каких-то девять месяцев СССР и США ставят подписи под Договором о запрещении ядерных испытаний в трех средах (атмосфере, космосе и под водой), вокруг которого несколько лет топтались переговорщики и находили многочисленные предлоги, почему «нельзя подписывать». А все потому, что не было политической воли лидеров, что не получали «сигнал сверху». Вскоре начинается работа над Договором о нераспространении ядерного оружия, чему не препятствует смена хозяина Белого дома после убийства Кеннеди. Понимание, что нельзя ставить судьбы своих стран, судьбы всего мира на грань ядерной катастрофы, пришло как раз в разгар Карибского кризиса. Совместные советско-американские усилия по предотвращению распространения ядерного оружия вкупе с двусторонне выстроенной системой ядерного сдерживания и архитектурой контроля над вооружениями позволили избежать сползания к бездне.

Конечно, нельзя игнорировать колоссальные различия между ядерным и кибероружием. Как справедливо замечает Игорь Иванов, «ядерное оружие создавалось и развертывалось не в целях последующего применения, а для сдерживания потенциальных противников. Страх глобальной ядерной войны предполагал максимальную осторожность и высокую ответственность ядерных держав. С кибероружием дело обстоит иначе – мало кто сейчас считает, что его применение создает непосредственную угрозу всему человечеству. А потому соблазн применить может оказаться слишком большим. При этом кибероружие в значительной степени анонимно, кибератака может быть произведена практически из любой точки планеты, и реальный киберагрессор останется неопознанным, а следовательно – и ненаказанным».

Страх перед кибероружием не синонимичен страху перед оружием ядерным. Но он тоже велик, и нарастает, и особенно мучителен как раз потому, что нет того «золотого петушка», который позволил бы легко определить, с какой стороны – с запада ли, с востока или еще откуда – «лезет рать».

Ощущение, что по «невидимым сетям» вероятный противник (будь то негосударственный субъект или, с большей вероятностью, государство) может накрыть и системы управления ядерным оружием, и личные электронные почтовые ящики влиятельных лиц, и системы подсчета голосования, и объекты критической инфраструктуры, кого-то вводит в ступор, кого-то доводит до паранойи, а кого-то подталкивает к планированию зеркальных или асимметричных ответных действий «на поражение». Око за око, зуб за зуб. Даже если и око, и зуб – виртуальные. Хотя грань-то между виртуальным и реальным как раз и размывается, и так недалеко до того, чтобы остаться слепым да беззубым. Именно ощущение вот этой новой уязвимости – сродни ощущению времен Карибского кризиса – я все больше замечаю и в Вашингтоне, и за его пределами.

Я не хотел бы сейчас гадать по поводу того, что произошло или не произошло в 2016 г. в отношении подготовки к американским президентским выборам. Для меня очевидно, что американские избиратели выбор сделали не под «внешним» влиянием, а исходя из собственных убеждений. Те, кто думают иначе, не уважают свой народ, считая, что он настолько подвержен манипуляциям. Вообще «российская угроза», «российский след» для многих в Вашингтоне сегодня не более чем удобный повод «поквитаться» с внутриполитическими оппонентами. Поляризация американских элит зашла так далеко, что для драки здесь любые средства хороши. А Россия просто удобно попалась под руку.

Но в то же время настороженность в отношении кибервозможностей России – реальный фактор американской внутренней и внешней политики. Он присутствует не только в стане демократов, но и среди республиканцев, которых сегодня кто-то наивно причисляет к «русофилам». Ее причина – куда глубже, чем попытка докопаться до ответа на вопрос, вмешивалась ли Россия в американские выборы. Ее причина – как раз в чувстве новой уязвимости. Россия не вмешивалась, но ведь могла вмешаться и еще может. Ощущение новой уязвимости требует ответа. Инстинктивная реакция – введение санкций. Однако санкциями кибервойны не остановить. Зато они могут подлить масла в огонь.

НА ВОЙНЕ КАК НА ВОЙНЕ

Кибервойна уже идет. Кто-то не заметил? Впрочем, неудивительно, что не заметили. Потому что это преимущественно невидимая война. Именно такая, какой и положено быть кибервойне.

Российские специалисты уже довольно давно определили характеристики таких кибервойн. Они, в частности, обратили внимание на необычайную сложность задач тактического предупреждения и оценки ущерба: «Существует реальная возможность того, что представленные национальному военно-политическому руководству оценки правоохранительных органов и разведывательных служб по конкретным случаям воздействия или ситуациям будут довольно противоречивы. Нападающая сторона, используя информационное оружие, способна с беспрецедентной оперативностью проводить стратегические операции и после выполнения задач мгновенно возвращаться в установленные пределы киберпространства».

По мнению российских специалистов, для проведения операций по дестабилизации внутреннего положения государства-противника наиболее эффективным каналом являются СМИ. При этом «могут применяться различные способы оказания воздействия через СМИ, в том числе и связанные с воздействием на инфраструктуру самих СМИ; оказание воздействия через национальные СМИ противника; в случае, если это невозможно, а также в целях достижения большего эффекта – формирование альтернативных каналов информационно-психологического воздействия (альтернативные СМИ, иновещание, (...) интернет); оказание внешнего давления на политическое руководство и общественное мнение государства-противника, создание международного климата, препятствующего реализации планов противника».

При этом подавление существующих систем национального вещания, например уничтожение ретрансляционных спутников, телевизионных и радиовещательных станций специалисты относят к наименее эффективным методам в сравнении с вышеперечисленными.

Диалог по кибервопросам становится проблематичным в условиях кровожадной внутриполитической борьбы в США. В этой связи неудивительно, что ряд американских экспертов ожидает приме-

нения Россией киберорружия как неизбежности: око за око. Не как превентивного, но как ответного удара. Тем более там видят, что Россия способна все более эффективно и многопланово, к тому же асимметрично, действовать в информационном поле. Только в отличие от войны ядерной, здесь могут быть сотни тысяч незримых обменов ударами; правда, лишь немногие из них будут направлены на использование уязвимости сугубо военной; остальные – для использования уязвимости политической или психологической.

Раз война, значит крупнейшие американские *IT*-корпорации реагируют. В частности, создают «оперативные штабы», или *war rooms*. Первенство здесь принадлежит *Facebook* при участии принадлежащих этой компании *Instagram* и *WhatsApp*. В *war room* компании *Facebook* нет окон (в прямом смысле этого слова) и есть двадцать «борцов с фейковым проникновением», число которых со временем предполагается довести до двадцати тысяч. Как сказал Марк Цукерберг, выступая перед Конгрессом, «мы слишком поздно заметили [российское] вмешательство и теперь всеми силами стремимся упредить злоумышленников». По словам главы отдела кибербезопасности *Facebook*, «наша работа – засечь любого, кто попытается манипулировать общественным мнением. Найти и обезвредить».

О «борьбе» в киберпространстве объявил и ключевой союзник Соединенных Штатов – Великобритания. Причем устами обычно неразговорчивого руководителя МИ-6 Алекса Янгера. В своем программном выступлении по кибервопросам 3 декабря 2018 г. в шотландском университете Сент-Эндрюс глава МИ-6 заявил, что «борьба за киберпорядок» объявлена, и она ведется против «опытного оппонента, не связанного понятиями закона и морали». Хотя сначала имя этого «опытного оппонента» (или оппонентов) прямо не называлось, затем в выступлении прямо была указана Россия.

КАРИБСКИЙ КИБЕРКРИЗИС?

Время для диалога уходит. Американское «все позволено» уже наталкивается на серьезное противодействие, причем не только России, но и ее ключевого стратегического партнера в глобальных делах – Китая. Однако даже это пока не приводит американцев к понимаю не просто важности, но необходимости договариваться.

Напротив, принятая в 2018 г. Национальная стратегия для киберпространства США предполагает не только оборону, но и наступательные действия в отношении военной и киберинфраструктуры Китая и России. Ведущие американские специалисты с опытом работы на ключевых «киберпостах» в Пентагоне в эти дни дают такие рекомендации: «Соединенным Штатам следует дистанционно поражать инфраструктуру системы управления российскими вооруженными силами через заражение вирусами или посредством внедрения вредоносных объектов в эту систему через завербованных лиц. Потенциально США могли бы вырубить электроснабжение вокруг российских военных баз, с которых ведется российская кибердеятельность. Также можно было бы, в партнерстве с частными компаниями, выдавить русских из негосударственных интернет-сетей и закрыть элементы российского сегмента интернета».

Россия не может позволить себе закрыть глаза на такой сценарий. Как заметил недавно Сергей Нарышкин, «движимые химерами прошлого, Соединенные Штаты начинают все больше походить на самонадеянного библейского силача Голиафа, который, как известно, был повержен юным Давидом. (...) Важно прекратить безответственную игру на повышение ставок и отказаться от проецирования силы в межгосударственных отношениях. Не доводить дело до нового Карибского кризиса».

Готовясь к саммиту в Хельсинки в июле 2018 г., российская сторона подготовила проект Совместного заявления президентов России и США, где на первой же странице, третьим пунктом (следом за вопросами стратстабильности и нераспространения, а также терроризма) было предложено ориентировать профильные российские и американские государственные органы на продолжение и углубление проведенного обсуждения проблем незаконной деятельности в киберпространстве, принятие совместных и параллельных мер по недопущению дестабилизирующего воздействия на критическую инфраструктуру и внутренние политические процессы в наших странах, включая выборы. Как известно, совместного заявления в Хельсинки не приняли. Больше того, не было ни нового российско-американского саммита, ни даже содержательного разговора между президентами, когда многосторонние встречи в верхах сводили их вместе в Париже и Буэнос-

Айресе, так как по возвращении из Хельсинки Трамп столкнулся с угрозой обвинений в государственной измене.

Да, идут отдельные, порой не афишируемые, российско-американские встречи на экспертном уровне, в формате «второй» или «полуторной» дорожек. Последнее более продуктивно. Как со-организатор и участник одного из таких форматов, могу сказать, что российско-американская дискуссия по кибербезопасности, прошедшая в декабре прошлого года в Вене, при участии представителей нескольких международных организаций и помещенная в более широкий контекст стратегической стабильности, была, безусловно, полезной и интеллектуально стимулирующей. Однако без иллюзий: вырабатываемые такими форматами и площадками идеи могут быть востребованы, лишь когда общий климат в двусторонних отношениях потеплеет. Мы же наблюдаем дальнейшее падение температуры.

Риск перерастания нынешней ситуации в глобально-хаотичную кибервойну все больше тревожит международное сообщество. По словам генерального секретаря ООН Антониу Гутерриша, «злонамеренные действия в киберпространстве приводят к снижению доверия между государствами». В своей Повестке дня по разоружению генсек ООН призывает «безотлагательно выстроить международные меры доверия и повышенной ответственности в киберпространстве». Неужели, чтобы дойти до осознания важности «договариваться» по киберделам, шире – по всей повестке МИБ – придется пережить некий «Карибский киберкризис»? Или все это не более чем очередные модные «страшилки»?

Не хотелось бы впадать в фатализм. Но еще меньше хотелось бы принимать позу страуса, игнорируя тот очевидный факт, что – желают того крупнейшие мировые игроки или нет – но они к такому «Карибскому кризису» скатываются. Потому что кибервойна идет. Без правил. С высокой долей неопределенности. С раскручиваемой спиралью напряженности. С гонкой кибервооружений. И, конечно, нет никаких гарантий, что новый кризис будет контролируемым и приведет к «катарсису» в вопросах регулирования МИБ. Ведь только выпусти киберджинна из бутылки…

Поэтому усиливается тревожное ощущение, что новые – настоящие, а не «фейковые» – драматические события в киберпространстве еще только предстоят.